Access Control Policy

Gibble SaaS Platform

Prepared by: Gregory Ibbotson – G.I. IT Security

Version: 1.0

Leftorium Pty Ltd
Suite 204, 189E South Centre Road, Tullamarine VIC 3043
Email: info@gibble.com.au | Phone: (03) 9744 2887

ABN 65 7612 792
Trading as **Gibble** - *gibble.com.au*

Leftorium Pty Ltd (Trading as Gibble) Access Control Policy

Last updated: July 2025

Table of Contents

Leftorium Pty Ltd (Trading as Gibble) Access Control Policy

Last updated: July 2025

1. Purpose

1.1 This Access Control Policy ("Policy") outlines how Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), manages access to our SaaS platforms for learning, payroll, student management, and human resources management, as well as associated systems, data, and infrastructure. The Policy ensures that only authorised individuals access sensitive information and systems, protecting the confidentiality, integrity, and availability of personal information, customer data, and Gibble's operations.

1.2 The Policy aligns with our Security Policy (Sections 4 and 5) and supports compliance with applicable data protection and cybersecurity laws, including:

- Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth), particularly APP 11.
- EU General Data Protection Regulation 2016/679 (GDPR), Article 32.
- *Privacy Act 2020* (New Zealand), Information Privacy Principle (IPP) 5.
- Singapore Personal Data Protection Act (PDPA).
- California Consumer Privacy Act (CCPA/CPRA).
- Japan Act on the Protection of Personal Information (APPI).

1.3 For inquiries, contact our Security Officer at:

- **Email**: security@gibble.com.au
- **Address**: Level 2, Suite 204, 189E South Centre Rd, Tullamarine VIC 3043, Australia
- **Phone**: +61 3 9744 2887

1.4 This Policy is reviewed annually or as needed to reflect changes in regulations, technology, or business operations. Updates are posted at www.gibble.com.au/access-control.

2. Scope

2.1 This Policy applies to:

- All Gibble platforms, systems, and infrastructure, including those hosted on AWS (e.g., S3, RDS, EC2) and Microsoft Entra (e.g., Azure Blob Storage, Entra ID).
- Data processed through our Services, including personal information (e.g., names, contact details, biometric data), customer data, and analytics data, as described in the Privacy Policy (Section 4).
- All users, including corporate customers, their personnel, end users, employees, contractors, and third-party vendors accessing Gibble's systems.
- Physical access to Gibble's offices and hard-copy records.

2.2 It integrates with the Security Policy (Sections 4-6), Data Breach Response Plan (Section 7), and Acceptable Use Policy (Section 5) to ensure a cohesive approach to security and compliance.

Last updated: July 2025

3. Definitions

3.1 **Access**: The ability to view, modify, or interact with Gibble's systems, platforms, or data.

3.2 **Authorised User**: An individual (e.g., customer personnel, end user, employee, contractor) granted permission to access specific systems or data based on their role and need.

3.3 **Personal Information**: Information relating to an identified or identifiable individual, as defined in the Privacy Policy (Section 4).

3.4 **Role-Based Access Control (RBAC)**: A method of restricting access based on a user's role within the organisation or platform.

4. Access Control Principles

4.1 **Least Privilege**: Users are granted the minimum level of access necessary to perform their authorised tasks.

4.2 **Need-to-Know**: Access to sensitive data (e.g., biometric data, payroll records) is restricted to users with a legitimate business need.

4.3 **Segregation of Duties**: Critical tasks (e.g., system administration, data deletion) are assigned to different individuals to prevent unauthorised actions.

4.4 **Accountability**: All access is logged, monitored, and auditable to ensure traceability, as per the Security Policy (Section 4).

4.5 **Security by Design**: Access controls are embedded in system design and enforced through AWS IAM and Microsoft Entra.

5. Access Control Mechanisms

5.1 **Authentication**:

- **Multi-Factor Authentication (MFA)**: Required for all privileged accounts (e.g., system administrators, customer admins) and recommended for all users via Microsoft Entra ID and AWS IAM.
- **Strong Passwords**: Minimum 12 characters, including uppercase, lowercase, numbers, and special characters, enforced via Entra ID password policies.
- **Single Sign-On (SSO)**: Supported through Entra ID for seamless and secure access across platforms.
- **Biometric Authentication**: Used for physical office access and employee time tracking, with explicit consent (Privacy Policy, Section 19.2).

5.2 **Authorisation**:

- **Role-Based Access Control (RBAC)**: Access is assigned based on predefined roles, such as:

  - **Customer Admin**: Manages customer accounts, user permissions, and data uploads.
  - **End User**: Accesses platform features as defined by the customer.
  - **Employee/Contractor**: Accesses internal systems based on job function (e.g., IT, HR).
  - **Third-Party Vendor**: Limited access for specific tasks (e.g., support, development).
- **Attribute-Based Access Control (ABAC)**: Used for dynamic access decisions based on attributes (e.g., location, device compliance) via Entra ID conditional access policies.

5.3 **Encryption**:

- Access to data is protected by AES-256 encryption for data at rest and TLS 1.3 for data in transit, as per the Security Policy (Section 5.2).
- API access requires OAuth 2.0 tokens or API keys, managed securely via AWS API Gateway.

5.4 **Session Management**:

- Sessions expire after 15 minutes of inactivity, requiring re-authentication.
- Secure cookies and token-based authentication are used, as per the Cookie Policy (Section 4).

6. Access Management Processes

6.1 **Access Provisioning**:

- **Request Process**: Access requests are submitted to the IT Manager via a secure internal portal or email (security@gibble.com.au).
- **Approval**: Requests are approved by the Security Officer or customer admin, based on role and need-to-know.
- **Implementation**: Access is granted via AWS IAM or Entra ID, with MFA configured.

6.2 **Access Reviews**:

- Quarterly reviews of all user accounts to verify access levels and remove unnecessary permissions.
- Adlumin MDR and AWS CloudTrail provide access logs for audit purposes.

6.3 **Access Revocation**:

- Access is revoked immediately upon:
  - Termination of employment or contractor agreements.
  - Customer contract termination.
  - Detection of misuse, as per the Acceptable Use Policy (Section 6).
- Revocation is executed via Entra ID and AWS IAM, with confirmation logged.

6.4 **Emergency Access**:

- Temporary privileged access for emergency situations (e.g., system recovery) is granted via a break-glass account, monitored by Adlumin MDR.
- Emergency access requires approval from the Security Officer and CEO.

7. Physical Access Controls

7.1 **Office Access**:

- Gibble's Tullamarine, VIC office uses biometric locks and surveillance systems, as per the Security Policy (Section 11).
- Access is restricted to authorised employees and contractors, logged via a visitor management system.
- Hard-copy records are stored in secure cabinets with access limited to HR and authorised personnel.

7.2 **Data Centres**:

- AWS and Microsoft data centres employ biometric access, 24/7 security, and environmental controls, as per the Security Policy (Section 11.2).

8. Monitoring and Auditing

8.1 **Monitoring**:

- Adlumin MDR provides real-time monitoring of access attempts, detecting unauthorised access or anomalies.
- AWS CloudTrail and Microsoft Defender for Cloud log all access events, including API calls and login attempts.

8.2 **Auditing**:

- Quarterly access audits verify compliance with RBAC and least privilege principles.
- Annual third-party audits for ISO 27001 and SOC 2 Type II include access control reviews.
- Audit reports are available to customers upon request at security@gibble.com.au.

8.3 **Incident Detection**:

- Unauthorised access attempts are treated as security incidents, handled per the Data Breach Response Plan (Section 5).
- Adlumin MDR provides forensic analysis for access-related incidents.

9. Roles and Responsibilities

9.1 **Security Officer**:

- Oversees access control implementation and compliance.
- Approves or denies access requests.
- Investigates access violations with Adlumin MDR support.

9.2 **IT Manager**:

- Configures and maintains access controls in AWS IAM and Entra ID.
- Executes access provisioning and revocation.
- Conducts quarterly access reviews.

9.3 **Data Protection Officer (DPO)**:

- Ensures access controls comply with data protection laws.
- Handles data subject access requests related to personal information (Privacy Policy, Section 14).

9.4 **Customers**:

- Manage end-user access within their tenant environments.
- Ensure end users comply with access requirements (e.g., MFA, strong passwords).

9.5 **Employees and Contractors**:

- Use only authorised accounts and credentials.
- Report unauthorised access attempts to security@gibble.com.au within 1 hour, as per the Data Breach Response Plan (Section 5).

10. Compliance

10.1 This Policy aligns with:

- ISO 27001 A.9 (Access Control).
- GDPR Article 32 (Security of Processing).
- APP 11.1 (Security of Personal Information).
- NIST 800-53 AC-2 (Access Control).
- PDPA, CCPA/CPRA, and APPI security requirements.

10.2 AWS and Microsoft Entra compliance dashboards ensure adherence to these standards, with Adlumin MDR providing audit-ready access logs.

11. Training

11.1 All employees and contractors receive annual training on:

- Access control policies and procedures.
- Secure password management and MFA usage.
- Recognising and reporting unauthorised access attempts.

11.2 Customers are provided with guidance on managing end-user access during onboarding, as per the Acceptable Use Policy (Section 5).

12. Violations

12.1 Violations of this Policy (e.g., unauthorised access, sharing credentials) may result in:

- Immediate account suspension or revocation.
- Disciplinary action for employees or contractors.
- Contractual penalties for customers, as per the Acceptable Use Policy (Section 9).
- Reporting to regulators if the violation constitutes a data breach, per the Data Breach Response Plan (Section 8).

12.2 Violations are investigated by the Security Officer, with support from Adlumin MDR and the Data Breach Response Team.

13. Contact Information

13.1 For access control inquiries or to report violations, contact:

- **Security Officer**: security@gibble.com.au
- **Data Protection Officer**: privacy@gibble.com.au
- **Phone**: +61 3 9744 2887

13.2 Complaints can be escalated to:

- **Australia**: Office of the Australian Information Commissioner, enquiries@oaic.gov.au, 1300 363 992.
- **New Zealand**: Office of the Privacy Commissioner, enquiries@privacy.org.nz.
- **EU**: Relevant supervisory authority (e.g., ICO in the UK).
- **Singapore**: Personal Data Protection Commission, info@pdpc.gov.sg.
- **USA**: Relevant state authority (e.g., California Attorney General).

- **Japan**: Personal Information Protection Commission, info@ppc.go.jp.